



PUBLIC NOTICE

Federal Communications Commission
445 12th St., S.W.
Washington, D.C. 20554

News Media Information 202 / 418-0500
TTY 202 / 418-2555
Internet: <http://www.fcc.gov>

DA 10-62
Released: January 13, 2010

COMMENTS SOUGHT ON PRIVACY ISSUES
RAISED BY THE CENTER FOR DEMOCRACY AND TECHNOLOGY

NBP Public Notice # 29

PLEADING CYCLE ESTABLISHED

GN Docket Nos. 09-47, 09-51, 09-137

Comment Date: January 22, 2010

In order to inform the Commission's development of a National Broadband Plan, the Commission has inquired about the relevance of online privacy protections to broadband adoption and deployment. For example, in the Notice of Inquiry initiating the National Broadband Plan proceeding, the Commission asked "[w]hat are consumer expectations of privacy when using broadband services or technology and what impact do privacy concerns have on broadband adoption and use?"¹ The Commission has also solicited responses to questions about online privacy as it relates to cloud computing.²

The Center for Democracy and Technology recently filed a letter with significant questions about the use of personal information and privacy in an online, broadband world.³ The Commission seeks public comment on the questions and topics raised by the Center for Democracy and Technology in its letter, available at: <http://webapp01.fcc.gov/ecfs/document/view.action?id=7020365402>, and attached to this Public Notice.

This matter shall be treated as a "permit-but-disclose" proceeding in accordance with the Commission's *ex parte* rules. See 47 C.F.R. §§ 1.1200, 1.1206. Persons making oral *ex parte* presentations are reminded that memoranda summarizing the presentations must contain summaries of the substance of the presentations and not merely a listing of the subjects discussed. More than a one- or two-sentence description of the views and arguments presented generally is required. See 47 C.F.R. § 1.1206(b). Other rules pertaining to oral and written *ex parte* presentations in permit-but-disclose proceedings are set forth in section 1.1206(b) of the Commission's rules, 47 C.F.R. § 1.1206(b).

¹ *A National Broadband Plan for Our Future*, GN Docket No. 09-51, Notice of Inquiry, [24 FCC Rcd 4342](#), 4363, para. 59 (2009).

² *Comment Sought on Data Portability and Its Relationship to Broadband – NBP Public Notice #21*, GN Docket Nos. 09-47, 09-51, 09-137, Public Notice, [DA 09-2433](#) (Nov. 18, 2009).

³ [Letter](#) from Ari Schwartz, Vice President and COO, Center for Democracy & Technology, to Marlene H. Dortch, Secretary, FCC (Jan. 11, 2010) ("CDT Jan. 11, 2010 *Ex Parte*") at 2-3.

- All comments should refer to GN Docket Nos. 09-47, 09-51, and 09-137.
- Please title comments responsive to this Notice as “Comments —NBP Public Notice # 29.”
- Filers using the Commission’s Electronic Comment Filing System (ECFS) should enter the following text in the “Custom Description” field in the “Document(s)” section of the ECFS filing page: “Comments – NBP Public Notice #29”.

Comments may be filed using (1) the Commission’s Electronic Comment Filing System (ECFS), (2) the Federal Government’s eRulemaking Portal, or (3) by filing paper copies.⁴ Comments can be filed through the Commission’s ECFS filing interface located at the following Internet address: <http://www.fcc.gov/cgb/ecfs/>. Comments can also be filed via the Federal eRulemaking Portal: <http://www.regulations.gov>.⁵ In completing the transmittal screen, commenters should include their full name, U.S. Postal Service mailing address, and the applicable docket or rulemaking number. Parties who choose to file by paper must file an original and four copies of each filing. If more than one docket or rulemaking number appears in the caption of this proceeding, filers must submit two additional copies for each additional docket or rulemaking number.

Filings can be sent by hand or messenger delivery, by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail. All filings must be addressed to the Commission’s Secretary, Office of the Secretary, Federal Communications Commission.

- Effective December 28, 2009, all hand-delivered or messenger-delivered paper filings for the Commission’s Secretary must be delivered to FCC Headquarters at 445 12th St., SW, Room TW-A325, Washington, DC 20554. The filing hours are 8:00 a.m. to 7:00 p.m. All hand deliveries must be held together with rubber bands or fasteners. Any envelopes must be disposed of before entering the building. **Please Note:** The Commission’s former filing location at 236 Massachusetts Avenue, NE, Suite 110, Washington, DC 20002 permanently closed on December 24, 2009.
- Commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail) must be sent to 9300 East Hampton Drive, Capitol Heights, MD 20743.
- U.S. Postal Service first-class, Express, and Priority mail must be addressed to 445 12th Street, SW, Washington DC 20554.

People with Disabilities: To request materials in accessible formats for people with disabilities (Braille, large print, electronic files, audio format), send an e-mail to fcc504@fcc.gov or call the Consumer and Governmental Affairs Bureau at (202) 418-0530, (202) 418-0432 (TTY).

For further information about this Public Notice, please contact Randy Clarke at (202) 418-1500.

⁴ See Electronic Filing of Documents in Rulemaking Proceedings, 63 Fed. Reg. 24121 (1998).

⁵ Filers should follow the instructions provided on the Federal eRulemaking Portal website for submitting comments.

Attachment:

**Center For Democracy and Technology Letter
Filed January 11, 2009**



1634 Eye Street, NW
Suite 1100
Washington, DC 20006

January 11, 2009

FILED ELECTRONICALLY

Ms. Marlene H. Dortch
Secretary
Federal Communications Commission
445 Twelfth Street SW, Room TW-A325
Washington, DC 20554

RE: *Ex Parte* Presentation in Docket No. 09-51, 09-47, 09-137

Dear Ms. Dortch:

On January 5, 2010 I met with Blair Levin and Erik Garr of the National Broadband Plan team.

The discussion focused on how the Commission could get more public comment on protecting privacy and the use of personal information in broadband applications. Based on that discussion, I have created a draft Notice of Inquiry (NOI) for the Commission to consider releasing on this issue. This NOI is included below.

In accordance with Section 1.1206(b), 47 C.F.R. § 1.1206, this letter is being filed electronically with your office.

Respectfully Submitted,

Ari Schwartz
Vice President and COO



In the course of compiling the record for the Commission's development of the National Broadband Plan,¹ the Commission has invited comment on implementation of smart grid technologies, health delivery, open government and data portability. The Commission received comments regarding both the importance of the ability to utilize personal information and to protect personal privacy in each of these areas.

Accordingly, the Commission seeks more tailored comment on the use of personal information, identity management services, and privacy protection across broadband applications.

Meeting Consumer Expectations of Privacy. The Commission has received comments suggesting that the use of personal information remains central to the success of many of the technologies considered, yet trust in these technologies depends on the ability to meet basic consumer expectations of privacy. The Commission invites further comment on this issue, including:

1. What principles and standards should be considered to help articulate existing consumer expectations of privacy?
2. What can federal agencies do to help ensure that consumer expectations of privacy are met as new technologies platforms are developed?
3. Are there industry best practices or regulatory models that are useful in helping to ensure that can be adapted across technology platforms to ensure that users are protected while allowing for the proper use of personal information?

Building Privacy by Design. The Commission would like further comment on ways to promote the development of technologies that protect privacy as they also utilize data.

1. How can information be de-identified, encrypted, pseudonymized or used in the aggregate in ways that are useful to help protect privacy? How can the best of these methods be determined for a particular application?
2. What data minimization principles should be used for different types of data? How can these be built into the technology?
3. How can identity management systems be developed to help provide more direct user controls over personal information across platforms? In particular, how can these systems be designed so that the user is an equal partner to the relying party and the identity provider?
4. Are there existing technical standards that can help to promote privacy by design?

¹ See American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009) (Recovery Act).

5. What can the federal government do to help promote privacy by design?

Creation and Use of Transactional Data. Broadband applications create new sets of data about transactions including potentially the exact time, place and manner that could lead to the discovery of actions of individuals in public or in their homes. The Commission has received comments about concerns surrounding the collection, use and storage of this information and would appreciate further comment on this issue, including:

1. Are certain types of transactional data (location information, health data, etc) more sensitive than others? Should limits be placed on the retention or use of some of this data in ways that are not required today?
2. Are the current rules on government access and use of transactional data held by government agencies sufficient to ensure that this data cannot be abused?

Third-Party Applications. Many of the new platforms created for the use of broadband, such as those for energy grid and personal health records, would allow third party applications to be created to provide services for users. This use of third party applications has raised questions about the role of self-regulation and government regulation in promoting a trustworthy marketplace. The Commission would like further thoughts on the following areas:

1. What responsibilities do companies that create new platforms that vet third party applications create for themselves? Would holding the platform provider liable for the actions of third-party application that violate basic privacy and security standards create incentives to ensure that consumer privacy is protected? Would it stifle innovation? Is there a middle ground that can protect consumers and ensure innovation?